UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/829,674	04/10/2001	Katsuaki Akama	FUJA 18.570	1585

26304 7590 05/03/2006

KATTEN MUCHIN ROSENMAN LLP
575 MADISON AVENUE
NEW YORK, NY 10022-2585

EXAMINER	
PYZOCHA, MICHAEL J	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 05/03/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/829,674	**Applicant(s)** AKAMA, KATSUAKI	
	Examiner Michael Pyzocha	**Art Unit** 2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10 April 2006*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1 and 3-10* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1 and 3-10* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date *20060227*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

1. Claims 1 and 3-10 are pending.

2. Amendment filed 02/23/2005 has been received and considered.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claim 10 is rejected under 35 U.S.C. 103(a) as being unpatentable over Rowney (US 6373950) in view of Menezes et al (Handbook of Applied Cryptography) and further in view of Huang et al (US 6718274).

As per claim 10, Rowney a user terminal being able to communicate with a first server and a second server (see Fig. 1B); and wherein the first sever includes a proxy facility for executing authentication with the second server instead of the user terminal when receiving an identification information and a request for executing an authentication process from the user terminal (see column 14, lines 46-51); and the second server has an authentication facility to authenticate the user terminal in accordance with predetermined procedures and to provide a secret key for an authorized destination as a result of authentication (see column 19, lines 25-35); and wherein the user terminal comprises a transmitting unit to transmit the identification information used for identifying its own terminal and the request for executing the authentication process, to the first server, and a receiving unit to receive the secret information from the first server (see column 20, lines 7-17). The payment gateway computer is considered a part of the proxy server system.

Rowney fails to disclose the common key is encrypted using another common key and the smart card providing authentication, signatures and key exchange.

However, Menezes teaches such keys (see pages 15 and 552) and Huang et al discloses providing authentication, signatures and key exchange (see column 1 lines 41-53).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use a common key and to encrypt the common key and for the smartcard to include authentication, signatures and key exchange.

Motivation to do so would have been to allow for high rates of data throughput (see page 31) and to transport or store the key (see page 552) and because smartcards provide tamper-resistant storage for protecting private keys and other forms of personal information (see Huang et al column 1 lines 41-53).

5. Claims 1-2, 4-9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rowney (US 6373950), in view of Baskey et al (US 6732269) in view of Menezes et al (Handbook of Applied Cryptography) and further in view of Huang et al (US 6718274).

As per claim 1, Rowney discloses a user terminal and an electronic market server where authentication and encryption is used between the two (see column 4 lines 43-55), establishing means for establishing an encrypted communication session between the user terminal and the proxy server, using public and secret keys of the user terminal and an electronic signature both transmitted from the user terminal on column 14, lines 46-67 and on column 15, lines 1-5; and a proxy means for executing authentication of a certificate and exchanging a key between the proxy server and the electronic market server, using public/secret keys of the electronic market server on column 1 9, lines 25-43; and an information means for informing the key to the user terminal through the encrypted communication session and wherein an encrypted communication is executed between the user terminal and the electronic market server by using the key that was exchanged between the proxy server and the electronic market server" on column 14, lines 35-40 and 55-61. The customer computer system represents the user terminal. The merchant computer system represents the proxy server and the host legacy system in combination with the payment gateway system represent the proxy. The electronic signature is inherently present on the exchanged certificates. The payment gateway computer system is considered a part of the proxy/legacy server system because it provides reformatting functions that aid further functions of the proxy/legacy system towards authentication. It would have been obvious to one of ordinary skill in the art at the time of the invention to have the host legacy system in combination with the payment gateway system represent the proxy because they both work together towards the authentication of the client.

Rowney fails to disclose the proxy server being provided between a user terminal and an electronic market server and the shared key being a common key, which is encrypted using another common key and the smartcard providing authentication, signatures and key exchange.

However, Baskey et al teaches a proxy server between a client and a server (see column 5 lines 17-37), Menezes teaches a common key and encrypting the key (see pages 15 and 552) and Huang et al discloses providing authentication, signatures and key exchange (see column 1 lines 41-53).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use Baskey's proxy server between the client and merchant and for the client and merchant to use Menezes' common key and to encrypt the common key using a smartcard in Rowney's security method.

Motivation to do so would have been to provide scalable secure communications (see column 5 lines 17-37) and to allow for high rates of data throughput (see page 31) and to transport or store the key (see page 552) and because smartcards provide tamper-resistant storage for protecting private keys and other forms of personal information (see Huang et al column 1 lines 41-53).

With respect to Claim 4, the limitation of "wherein the home card comprises an information means for recording decision information regarding an electronic money in the home card and for informing the recorded decision information to a mail address of the user terminal" is met on column 108, lines 8-9, 13-33. The memory of the smart card makes the existence of an information means for recording decision information inherent in the reference.

With respect to Claim 5, the limitation of "wherein the home card comprises a cancel means for canceling the decision information in the home card based on an authentication information for canceling the decision, and for adding electronic money subtracted by the decision to the electronic money in the home card" is met on column 107, lines 45-57. The cancel means would have been obvious to one of ordinary skill in the art at the time of the invention because the electronic wallet in the reference has an interface that allows for reading and writing of information to itself. Because electronic money can be subtracted from the electronic wallet, so also would it be obvious to add electronic money to the wallet due to a canceled transaction/decision or simply just to transfer one's balance onto the wallet from a pre-existing account.

With respect to Claim 6, the limitation of "wherein the home card comprises a re-supplement means for supplementing the electronic money by adding supplementary electronic money, which was requested by the user terminal, to the electronic money in the home card, based on the authentication information in an electronic money managing facility provided in the proxy facility" is met inherently on column 107, lines 6 1-65 and on column 108, lines 16-22. Visa and debit cards are inherently forms of supplemental electronic money.

With respect to Claim 7, the limitation of "a proxy server and an electronic market server; the access card being connected to the user terminal; and the proxy server including a proxy facility being provided between the user terminal and the electronic market server for executing authentication and encryption to the electronic market server, instead of the user terminal; the access card" is met on column 4, lines 43-55 and on column 108, lines 7-22; and "an establishment means for establishing an encrypted communication session between the user terminal and the proxy server including the proxy facility" is met on column 14, lines 66-67 and on column 15, lines 1-8; and "an encrypted communication means for receiving a common key, which is exchanged between the proxy server and the electronic market server after an authentication process for the electronic market server, from the proxy server through the encrypted communication session, and for executing the encrypted communication with the electronic market server by using the common key" is met on column 19, lines 25-35 with the encrypted common key as applied above with the smartcard features taught by Huang et al in column 1 lines 41-53.

With respect to Claim 8, the limitation of "a reception unit to receive an identification information and a request for executing an authentication process, from the user terminal and a decision means for determining whether or not the identification information is stored in an internal or external memory" is met on column 14, lines 47-51, 55-61. The decision means is inherent from the fact that the merchant verifies the client's certificate. Further limitation of "a proxy means for executing a part, or all, communication in accordance with the predetermined procedures when the identification information is stored in the memory" is met on column 17, lines 45-49, 59-67 and on column 18, lines 1-4 with the encrypted common key as applied above with the smartcard features taught by Huang et al in column 1 lines 41-53.

With respect to Claim 9, its limitation is similar to Claim 8 limitation and hence its rejection can be found therein.

6. Claim 3 is rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Rowney, Baskey, Menezes, and Huang et al system and further in view of Mooney et al (US 6351813).

With respect to Claim 3, the modified Rowney, Baskey, Menezes and Huang et al system meets all the limitation except for the following limitation. The limitation of "wherein the home card includes a logic circuit which enables an access by using a first password input from the user terminal; and a security releasing means for releasing the security for the proxy means by using a second password input from the user terminal, after establishment of the encrypted communication session to the user terminal in which an access was permitted" is met by Mooney et al on column 1, lines 59-67, column 2, lines 1- 11 and on column 9, lines 31-36.

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the teachings of Mooney et al within the system of Rowney because a smart card and password combination system as a means of authentication is a well-known method of authentication in the art.

Response to Arguments

7. Applicant's arguments with respect to claims 1 and 3-10 have been considered but are moot in view of the new ground(s) of rejection.

8. Applicant's arguments filed 04/10/2006 have been fully considered but they are not persuasive. Applicant argues that the combined references fail to disclose direct communication between the user terminal and an electronic market server. With respect to this argument Applicant is directed to figure 1B where Rowney clearly shows a direct connection between the user terminal and the merchant server.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael Pyzocha whose telephone number is (571) 272-3875. The examiner can normally be reached on 7:00am - 4:30pm first Fridays of the bi-week off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MJP

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER